「個人情報の保護に関する法律施行規則の一部を改正する規則（案）」
に関する意見

2021年1月 25日

BSA｜ザ・ソフトウェア・アライアンス[1]（以下、「**BSA**」）は、令和 2 年 6 月に公布された改正個人情報保護法に関する「法律施行規則の一部を改正する規則（案）」（以下「**規則案**」）に関し、個人情報保護委員会（以下、**貴委員会**）に対して、以下のとおり意見を提出致します。

総論

BSA は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSA の会員は、世界で最もイノベーティヴな企業で構成されており、経済を活性化させるフトウェア・ソリューションを創造しています。BSA 会員企業 は、日本市場に多大な投資を行っており、BSA 会員企業提供の製品やサ ービスによって日本の多くの企業や消費者が日本経済を支えていることを誇りに思 っております。

BSA 会員は、ソフトウェアが可能とする製品やサービスを創造し、他のビジネスを強化するエンタープライズ・ソリューション・プロバイダーです。クラウドストレージサービス、カスタマー・リレーションシップ・マネジメント（CRM）・ソフトウェア、人事管理プログラム、ID 管理サービス、サイバーセキュリティ・ソリューション、コラボレーション・ソフトウェアなどのツールを提供しています。これらのエンタープライズ・ソフトウェア企業の事業は、プライバシーが保護されたソリューションの提供であり、ユーザーのデータを収益化するビジネスモデルではありません。BSA 会員は、企業は消費者の信頼を得て、個人データの取り扱いに責任を持って行動しなければならないと認識しています。

[1] BSA の活動には、Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workdayが会員企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

我々は、個人データの保護と利活用に関する国際的な議論をリードする貴委員会の献身的な取り組みに感謝し、今後も適切な国際的枠組みを通じて、貴委員会が国際的な個人情報保護制度の調和と相互運用性を促進し続けることを奨励致します。

BSA 会員企業は、テクノロジーやビジネスモデルを通して、個人データを保護することに長年、深くコミットしております。テクノロジーの利用者は、自身の個人データに関する企業の管理を信頼して初めて、新たなテクノロジーの恩恵を安心して受けることができると認識しているからです。BSA は以前、2020 年 1 月の「個人情報保護法　いわゆる 3 年ごと見直し　制度改正大綱」[2]について意見を提出しており（以下「**前回意見書**」）、本意見書ではその内容を取り上げています。BSA は、改正個人情報保護法の施行に向けて検討されている方向性を注視しており、今回の改正で影響を受けるステークホルダーとの議論の機会を貴委員会が設けてくださったことに感謝しております。

BSA は、各国における個人データ保護法の実施に関し、以下を世界的に提唱しています：個人データの収集・利用の透明性の向上、その収集と利用に関するガバナンスを通じて十分な情報に基づいた選択を尊重・可能とすること、消費者による自らの個人データの管理、強固なセキュリ ティの実践、正当な事業目的のためのデータ利用促進 [3]。BSA はまた、各国の個人データ保護制度の国際的な相互運用性を提唱しています。これはデジタル経済に不可欠な要素であり、これにより個人データの国際的な移転が可能となり促進されます。様々なプライバシー体制において差異がある場合、BSA は、プライバシー保護とデータの自由な移転の促進を両立させながら、その違いを埋める手段を策定することを各国政府に奨励しています。[4]

提言

漏えい等報告・本人通知 / 規則案　第六条の二、六条の三 、六条の五

BSA は、漏えい等に関し、貴委員会が我々の前回意見書を考慮に入れて頂き、暗号化されたデータを適用除外とし、損害を生じさせる重大なリスクがある場合のみに報告・通知要件を限定したことを歓迎します。また、速報の提出に特定の期限を設けず、確報の提出に合理的な時間を設けたことも支持します。このようなアプローチにより、影響を受けた事業者がセキュリティ・リスクの範囲を特定するリスク評価を実施し、対応策に着手し、インシデントの再発防止策を策定することが可能となります。また、貴委員会 への報告と同タイミングで関連する本人への通知を要件としない提案も支持します。

[2] https://bsa.or.jp/wp-content/uploads/20200117j.pdf
[3] BSAの「 Global Privacy Best Practices」に関しては以下を参照ください。
https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf
[4] BSA の「Privacy Framework」に関しては以下を参照ください。
https://www.bsa.org/policy-filings/bsa-privacy-framework

なお、規則案の中で、貴委員会 に提出された速報に第六条の三第 一項第 一 号から第九 号までのすべての情報が含まれている場合には、これも第六条の三第二 項で要求される確定報告となり、追加の確定報告は不要であることを明確にして頂くことを奨めます。

また、規則案に含まれる「発生したおそれがある」といった、個人データ漏えいの「可能性がある」事態を報告・通知要件に含むことについては、引き続き懸念を抱いております。漏えい等が確認された後、可能な限り速やかに対策を講じなければならないことには同意しますが、このような報告・通知は、漏えい等が発生し、暗号化されていない個人データや再加工されていない個人データが実際に不正取得され、なりすまし犯罪や金融詐欺など、本人にとって重大なリスクが生じる場合に限定すべきです。このようなアプローチにより、セキュリティ・インシデントを分析し、それが漏えい等として分類されるべきかどうかを判断することが可能となり、このようなインシデントから生じる結果的な被害に対処するための、産業界と貴委員会の限られたリソースが賢明に活用されることを確実にします。実際には発生していないかもしれない「可能性のある漏えい等」の報告・通知を要求することは、組織に負担をかけるだけでなく（インシデント対応は時間とリソースがかかるため）、貴委員会への報告が殺到し、また、当該本人にとっては、取るに足らないデータ・セキュリティ・インシデント（例えば、暗号化されたデータへの不正アクセスなど）と、重大な被害をもたらす可能性があり、適切な是正措置を取るべき漏えい等との区別がつかない情報が氾濫することとなります。したがって、我々は、「可能性がある」データ・インシデントを報告するという要件の提案は、個人データ漏えい等に対する個人の保護を実質的に強化するものではないため、規則案から削除することを求めます。

また、規則案第六条の三第一項第五号の「二次被害又はそのおそれの有無及びその内容」の報告義務についても懸念しております。特に他の事業者に代わってデータ処理を行う事業者は、二次被害があったかどうかを測ることができないことが多く、又、二次被害が発生する可能性のある不測の事態や未知の事態もあり得るため、二次被害が発生していないかもしれないと推測し、そのように報告することも適切ではありません。加えて、二次被害が発生する可能性がある場合でも、二次被害が発生する**確率**が低い可能性があります。本人にも同じ情報を提供する必要があることから、本人に不必要な不安を与え、有意義な通知から目をそらしてしまい、結果的にどちらの場合にも対応を取らなくなる可能性を生じさせてしまいます。このような懸念に対応する上でも、第六条の三第一項第五号を改正し、「二次被害が**発生した場合**又は二次被害の**合理的な危険性がある場合**及びその内容」の報告に限定した要件とすることを求めます。

また、例えば、事業者が漏えい等の影響を受けた個人の連絡先情報を有していない等、関係する個人への通知が困難である場合について、貴委員会で通知の代替手段を検討していただくことを引き続き求めます。ある状況においては、事業者が漏えい等の影響を受けた本人に直接連絡を行うよりも貴委員会に報告する方が適している場合があります。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

越境データ移転 ／ 規則案　第十一条の三

上記に関し、事業者は、本人同意を得る必要がある場合には、以下の情報を本人に提供しなければならないと理解しています：（１）移転先の外国名称、（２）移転先国における個人情報保護に関する制度、（３）提供先の第三者が講ずる個人情報の保護のための措置。

このような要件は、前回意見書で強調したように、自身の個人情報の取り扱いに関して本人の理解を深める、という貴委員会 の目標を達成できない可能性があります。データセキュリティと個人情報保護の有効性は、データが物理的に保管または処理される場所とはあまり関係がなく、代わりに、個人情報を取り扱う事業者、およびデータを受け取る第三者が、強固なセキュリティ対策を提供することを含めて実施するテクノロジー、システム、および手順の質に依存しています。事業者は、国内外を問わず、移転されるすべての個人データについて説明責任を負うべきです。例えば、個人情報の提供先の第三者が EU 域外の国に本社を置いている場合でも、その事業者は、データがどこから来たか、データがどこで保管・処理されているかに関わらず、その事業者が処理するすべてのデータに （日本が十分性認定をした）EU のデータ保護法を適用する選択をすることもあります。このように、個人情報がどこで保管・処理されているか、あるいは第三者の処理者がどこに本社を置いているかは、データ処理の方針や手順よりも重要ではありません。そのようなことから、海外事業者を含む企業が個人情報をどのように保護しているかについて理解することの重要性を、貴委員会から個人に向けて指導していただき、国内での個人情報の取扱いと比較して、外国にある第三者の提供先の方がセキュリティ・リスクが高いという誤解が生じないようにして頂くことを求めます。

そして、貴委員会が越境データ移転に本要件を課すことを決定したことを踏まえ、第十一条の三 における「外国」の定義を、データの提供先である第三者が本社を置く国を指すものとすることを明確にして頂きたく思います。貴委員会からのこれまでの説明に基づき、規則案における「外国」とは、データの移転先である第三者が本社を置く国であって、データを物理的に保管または処理するために使用されるデータセンターが所在する国ではないと理解しています。したがって、混乱を避けるためにも、規則案では、上記のように「外国」を明確に定義することを推奨します。

越境データ移転 ／ 規則案　第十一条の四

改正個人情報保護法第二十四条第三項に基づき、規則案第十一条の四は、委員会規則で定める基準に適合した体制整備を根拠とした個人データの越境移転について、事業者は、海外の第三者が国内の事業者と同等の措置を継続的に講じていること、及び「外国」のデータ保護体制が当該データ保護措置の実施を不当に阻害していないことを定期的に確認する必要があると規定しています。 これにより、移転された個人情報は、海外の第三者による同等の措置により保護され続けることになります。

貴委員会からの説明では、この要件は 一年に 一回満たす必要があると理解しております。
我々は貴委員会がこのような合理的な対応を考慮に入れたことを支持するとともに、今後の改正個人情報保護法に関 するガイドライン（以下「**ガイドライン**」）において、この要求事項を遵守するために、どのような報告が適切であると考えられるかを明確にすることを奨めます。

仮名加工情報／規則案　第十八条の七

第十八条の七に規定されている基準は、仮名加工情報の作成方法を判断する上で有用であり、今後のガイドラインの中で、事業者が参考にできる例を貴委員会が提示するという理解でおります。ガイドラインにおいては、「例」は例示的なものであることを明確にして頂き、追加情報を使用せずに特定のデータ主体に帰することができない限り、事業者が個人データを仮名化するにあたり、別の手段を採用し続けること可能にして頂くことを求めます。

結語

BSA は、規則案に意見を提出する機会に感謝します。本意見が、新たな要件をより明確にするために、規則を修正し、今後ガイドラインを策定する上での貴委員会の引き続きの検討に有用であれば幸いです。施行規則の策定において、貴委員会が複数のステークホルダーを関与させ、進捗状況を共有する過程をとって頂いたことに感謝致します。本意見に関して、ご質問がある場合又はより詳細に議論をされたい場合には是非ご連絡下さい。